# i.MX8 SHE API Rev 0.1 NXP Copyright

Generated by Doxygen 1.8.17

2 Revision History

1 SHE API	1
2 Revision History	1
3 General concepts related to the API	2
3.1 Session	2
4 Module Index	2
4.1 Modules	2
5 Module Documentation	2
5.1 Session	2
5.1.1 Detailed Description	3
5.1.2 Data Structure Documentation	3
5.1.3 Macro Definition Documentation	3
5.1.4 Typedef Documentation	4
5.1.5 Function Documentation	4
5.2 Key store	7
5.2.1 Detailed Description	7
5.2.2 Macro Definition Documentation	7
5.2.3 Function Documentation	8
5.3 Utils	10
5.3.1 Detailed Description	10
5.3.2 Data Structure Documentation	10
5.3.3 Function Documentation	10
5.4 Shared Buffer	12
5.4.1 Detailed Description	12
5.4.2 Data Structure Documentation	12
5.5 Error codes	13
5.5.1 Detailed Description	13
5.5.2 Enumeration Type Documentation	13
Index	15

# 1 SHE API

This document is a software referece description of the API provided by the i.MX8 SHE solutions.

# 2 Revision History

Revision	date	description	
0.1	Jul 06 2023	first draft	

# 3 General concepts related to the API

## 3.1 Session

The API must be initialized by a potential requestor by opening a session.

The session establishes a route (MU, DomainID...) between the requester and the SHE module, and grants the usage of a specified key store. When a session is opened, the SHE module returns a handle identifying the session to the requester.

## 4 Module Index

## 4.1 Modules

Here is a list of all modules:

Session	2
Key store	7
Utils	10
Shared Buffer	12
Error codes	13

## 5 Module Documentation

## 5.1 Session

## **Data Structures**

· struct she\_hdl\_s

#### **Macros**

- #define SHE\_HANDLE\_NONE (0x0)
- #define SHE\_MAX\_SESSIONS (16u)
- #define SHE\_OPEN\_SESSION\_PRIORITY\_LOW (0x00U)
- #define SHE\_OPEN\_SESSION\_PRIORITY\_HIGH (0x01U)
- #define SHE OPEN SESSION FIPS MODE MASK BIT(0)
- #define SHE\_OPEN\_SESSION\_EXCLUSIVE\_MASK BIT(1)
- #define SHE\_OPEN\_SESSION\_LOW\_LATENCY\_MASK BIT(3)
- #define SHE\_OPEN\_SESSION\_NO\_KEY\_STORE\_MASK BIT(4)

### **Typedefs**

typedef uint32\_t she\_hdl\_t

5.1 Session 3

### **Functions**

- struct she\_hdl\_s \* she\_session\_hdl\_to\_ptr (uint32\_t hdl)
- void delete\_she\_session (struct she\_hdl\_s \*s\_ptr)
- struct she hdl s \* add she session (void)

## 5.1.1 Detailed Description

### 5.1.2 Data Structure Documentation

## **5.1.2.1 struct she\_hdl\_s** Structure describing the session handle members

**Data Fields** 

struct plat_os_abs_hdl *	phdl	Pointer to OS device node.	
uint32_t session_handle		Session handle.	
uint32_t key_store_handle		handle to access key store	
uint32_t	cipher_handle	handle to access cipher services	
uint32_t	rng_handle	RNG handle.	
uint32_t utils_handle		handle to access utility	
uint32_t mu_type		Session MU type.	

## 5.1.3 Macro Definition Documentation

5.1.3.1 SHE\_HANDLE\_NONE #define SHE\_HANDLE\_NONE (0x0)

Handle not available

5.1.3.2 SHE\_MAX\_SESSIONS #define SHE\_MAX\_SESSIONS (16u)

Maximum sessions supported

5.1.3.3 SHE\_OPEN\_SESSION\_PRIORITY\_LOW #define SHE\_OPEN\_SESSION\_PRIORITY\_LOW (0x00U)

Session opening priority flags Low priority. default setting on platforms that doesn't support sessions priorities.

5.1.3.4 SHE\_OPEN\_SESSION\_PRIORITY\_HIGH #define SHE\_OPEN\_SESSION\_PRIORITY\_HIGH (0x01U) High Priority session.

5.1.3.5 SHE\_OPEN\_SESSION\_FIPS\_MODE\_MASK #define SHE\_OPEN\_SESSION\_FIPS\_MODE\_MASK BIT(0)

Operating Mode Only FIPS certified operations authorized in this session.

```
5.1.3.6 SHE_OPEN_SESSION_EXCLUSIVE_MASK #define SHE_OPEN_SESSION_EXCLUSIVE_MASK BIT(1)
```

No other SHE session will be authorized on the same security enclave.

```
5.1.3.7 SHE_OPEN_SESSION_LOW_LATENCY_MASK #define SHE_OPEN_SESSION_LOW_LATENCY_MA  
SK BIT(3)
```

Use a low latency SHE implementation.

```
5.1.3.8 SHE_OPEN_SESSION_NO_KEY_STORE_MASK #define SHE_OPEN_SESSION_NO_KEY_STORE_MA↔ SK BIT(4)
```

No key store will be attached to this session. May provide better performances on some operation depending on the implementation. Usage of the session will be restricted to operations that doesn't involve secret keys (e.g. hash, signature verification, random generation)

## 5.1.4 Typedef Documentation

```
5.1.4.1 she_hdl_t typedef uint32_t she_hdl_t
```

Define the SHE handle type

## 5.1.5 Function Documentation

```
5.1.5.1 she_session_hdl_to_ptr() struct she_hdl_s* she_session_hdl_to_ptr ( uint32_t hdl )
```

Returns pointer to the session handle

## **Parameters**

hdl identifying the session handle.

## Returns

pointer to the session handle.

```
5.1.5.2 delete_she_session() void delete_she_session ( struct she_hdl_s * s_ptr)
```

5.1 Session 5

Delete the session

## **Parameters**

*s\_ptr* pointer identifying the session.

Add the session

## Returns

pointer to the session.

5.2 Key store 7

## 5.2 Key store

User must open a key store service flow in order to perform the following operations:

#### **Macros**

- #define MIN\_MAC\_LEN\_NOT\_SET BIT(0)
- #define MIN MAC LEN SET BIT(1)
- #define KEY\_STORE\_OPEN\_FLAGS\_DEFAULT 0x0u
- #define KEY STORE OPEN FLAGS CREATE 0x1u
- #define KEY\_STORE\_OPEN\_FLAGS\_SHE 0x2u
- #define KEY STORE OPEN FLAGS SET MAC LEN 0x8u
- #define KEY\_STORE\_OPEN\_FLAGS\_STRICT\_OPERATION 0x80u
- #define SHE STORAGE CREATE SUCCESS 0u
- #define SHE STORAGE CREATE WARNING 1u
- #define SHE STORAGE CREATE UNAUTHORIZED 2u
- #define SHE\_STORAGE\_CREATE\_FAIL 3u
- #define SHE\_STORAGE\_NUMBER\_UPDATES\_DEFAULT 300u
- #define SHE\_STORAGE\_MIN\_MAC\_BIT\_LENGTH\_DEFAULT 32u

#### **Functions**

she\_err\_t she\_open\_key\_store (she\_hdl\_t session\_hdl, open\_svc\_key\_store\_args\_t \*args)

## 5.2.1 Detailed Description

User must open a key store service flow in order to perform the following operations:

- · create a new key store
- perform operations involving keys stored in the key store (ciphering, signature generation...)
- perform a key store reprovisioning using a signed message. A key store re-provisioning results in erasing all the key stores handled by the SHE.

To grant access to the key store, the caller is authenticated against the domain ID (DID) and Messaging Unit used at the keystore creation, additionally an authentication nonce can be provided.

#### 5.2.2 Macro Definition Documentation

## 5.2.2.1 MIN MAC LEN NOT SET #define MIN\_MAC\_LEN\_NOT\_SET BIT(0)

Minimum mac length not set

## 5.2.2.2 MIN\_MAC\_LEN\_SET #define MIN\_MAC\_LEN\_SET BIT(1)

Minimum mac length is set

5.2.2.3 KEY\_STORE\_OPEN\_FLAGS\_DEFAULT #define KEY\_STORE\_OPEN\_FLAGS\_DEFAULT 0x0u default flags

**5.2.2.4 KEY\_STORE\_OPEN\_FLAGS\_CREATE** #define KEY\_STORE\_OPEN\_FLAGS\_CREATE 0x1u Create a key store

5.2.2.5 KEY\_STORE\_OPEN\_FLAGS\_SHE #define KEY\_STORE\_OPEN\_FLAGS\_SHE 0x2u

Target key store is a SHE key store

5.2.2.6 KEY\_STORE\_OPEN\_FLAGS\_SET\_MAC\_LEN #define KEY\_STORE\_OPEN\_FLAGS\_SET\_MAC\_LEN 0x8u Check min mac length

5.2.2.7 KEY\_STORE\_OPEN\_FLAGS\_STRICT\_OPERATION #define KEY\_STORE\_OPEN\_FLAGS\_STRICT\_OP  $\leftarrow$  ERATION 0x80u

The request is completed only when the key store has been written in the NVM and the monotonic counter has been updated. This flag is applicable for CREATE operation only

**5.2.2.8 SHE\_STORAGE\_CREATE\_SUCCESS** #define SHE\_STORAGE\_CREATE\_SUCCESS Ou New storage created successfully.

**5.2.2.9 SHE\_STORAGE\_CREATE\_WARNING** #define SHE\_STORAGE\_CREATE\_WARNING 1u New storage created but its usage is restricted to a limited security state of the chip.

**5.2.2.10** SHE\_STORAGE\_CREATE\_UNAUTHORIZED #define SHE\_STORAGE\_CREATE\_UNAUTHORIZED 2u Creation of the storage is not authorized.

**5.2.2.11** SHE\_STORAGE\_CREATE\_FAIL #define SHE\_STORAGE\_CREATE\_FAIL 3u Creation of the storage failed for any other reason.

**5.2.2.12 SHE\_STORAGE\_NUMBER\_UPDATES\_DEFAULT** #define SHE\_STORAGE\_NUMBER\_UPDATES\_DEFAU←
LT 300u

default number of maximum number of updated for SHE storage.

5.2.2.13 SHE\_STORAGE\_MIN\_MAC\_BIT\_LENGTH\_DEFAULT #define SHE\_STORAGE\_MIN\_MAC\_BIT\_LENG 

TH\_DEFAULT 32u

default MAC verification length in bits

## 5.2.3 Function Documentation

Open a service flow on the specified key store.

5.2 Key store 9

# **Parameters**

session_hdl	pointer to the handle identifying the current session.	
args	pointer to the structure containing the function arguments.	

## Returns

error code.

## 5.3 Utils

User must open a SHE utils service flow in order to perform the following operations:

### **Data Structures**

· struct op\_open\_utils\_args\_t

### **Functions**

• she\_err\_t she\_open\_utils (she\_hdl\_t session\_hdl, op\_open\_utils\_args\_t \*args)

## 5.3.1 Detailed Description

User must open a SHE utils service flow in order to perform the following operations:

- · Create a utils handle
- · perform SHE key update extension
- update SHE plain key
- · export SHE plain key
- get SHE identity (UID)
- · get SHE status register
- perform MAC generation and verification in fast mode for a SHE session on V2X
- perform MAC generation and verification in fast mode for a SHE session

## 5.3.2 Data Structure Documentation

**5.3.2.1 struct op\_open\_utils\_args\_t** Structure describing the open utils service operation arguments

**Data Fields** 

```
uint32_t utils_handle
```

### 5.3.3 Function Documentation

Open SHE utils service flow on the specified key store. The SHE utils service flow can be opened only after opening SHE key storage handle.

5.3 Utils 11

# **Parameters**

session_hdl	pointer to the handle identifying the current session.	
args	pointer to the structure containing the function arguments.	

## Returns

error code.

# 5.4 Shared Buffer

## **Data Structures**

• struct op\_shared\_buf\_args\_t

# 5.4.1 Detailed Description

# 5.4.2 Data Structure Documentation

# **5.4.2.1 struct op\_shared\_buf\_args\_t** Structure describing the get shared buffer operation arguments

## **Data Fields**

uint16_t	shared_buf_offset	et offset of the shared buffer in secure memory	
uint16_t	shared_buf_size	size in bytes of the allocated shared buffer	

5.5 Error codes 13

## 5.5 Error codes

Error codes returned by SHE functions.

### **Enumerations**

```
enum she_err_t {
 SHE_NO_ERROR = 0x0,
 SHE\_SEQUENCE\_ERROR = 0x1,
 SHE_KEY_NOT_AVAILABLE = 0x2,
 SHE_KEY_INVALID = 0x3,
 SHE_KEY_EMPTY = 0x4,
 SHE_NO_SECURE_BOOT = 0x5,
 SHE KEY WRITE PROTECTED = 0x6,
 SHE_KEY_UPDATE_ERROR = 0x7,
 SHE_RNG_SEED = 0x8,
 SHE NO DEBUGGING = 0x9,
 SHE BUSY = 0xA,
 SHE_MEMORY_FAILURE = 0xB,
 SHE\_GENERAL\_ERROR = 0xC,
 SHE_UNKNOWN_WARNING = 0x27,
 SHE_FATAL_FAILURE = 0x29 }
```

## 5.5.1 Detailed Description

Error codes returned by SHE functions.

## 5.5.2 Enumeration Type Documentation

```
5.5.2.1 she_err_t enum she_err_t
```

Error codes returned by SHE functions.

## Enumerator

SHE_NO_ERROR	Success.
SHE_SEQUENCE_ERROR	Invalid sequence of commands.
SHE_KEY_NOT_AVAILABLE	Key is locked.
SHE_KEY_INVALID	Key not allowed for the given operation.
SHE_KEY_EMPTY	Key has not beed initialized yet.
SHE_NO_SECURE_BOOT	Conditions for secure boot process are not met.
SHE_KEY_WRITE_PROTECTED	Memory slot for key has been write-protected.
SHE_KEY_UPDATE_ERROR	Key update failed due to errors in verification of the messages.
SHE_RNG_SEED	The seed has not been initialized.
SHE_NO_DEBUGGING	Internal debugging is not possible.
SHE_BUSY	A function of SHE is called while another function is still processing.
SHE_MEMORY_FAILURE	Memory error (e.g. flipped bits).
SHE_GENERAL_ERROR	Error not covered by other codes occurred.
SHE_UNKNOWN_WARNING	SHE Unknown Warning.
SHE_UNKNOWN_WARNING Generated by Doxygen SHE_FATAL_FAILURE	A fatal failure occurred, SHE goes in unrecoverable error state not replying to further requests

## Index

```
add_she_session
                                                  Key store, 7
    Session, 6
                                              op_open_utils_args_t, 10
delete she session
                                              op_shared_buf_args_t, 12
    Session, 4
                                              Session, 2
                                                  add she session, 6
Error codes, 13
                                                  delete she session, 4
    SHE BUSY, 13
                                                  SHE_HANDLE_NONE, 3
    she err t, 13
                                                  she hdl t, 4
    SHE_FATAL_FAILURE, 13
                                                  SHE MAX SESSIONS, 3
    SHE_GENERAL_ERROR, 13
                                                  SHE_OPEN_SESSION_EXCLUSIVE_MASK, 3
    SHE_KEY_EMPTY, 13
                                                  SHE_OPEN_SESSION_FIPS_MODE_MASK, 3
    SHE KEY INVALID, 13
                                                  SHE_OPEN_SESSION_LOW_LATENCY_MASK,
    SHE_KEY_NOT_AVAILABLE, 13
    SHE_KEY_UPDATE_ERROR, 13
                                                  SHE_OPEN_SESSION_NO_KEY_STORE_MASK,
    SHE KEY WRITE PROTECTED, 13
    SHE MEMORY FAILURE, 13
                                                  SHE OPEN SESSION PRIORITY HIGH, 3
    SHE NO DEBUGGING, 13
                                                  SHE OPEN SESSION PRIORITY LOW, 3
    SHE NO ERROR, 13
                                                  she_session_hdl_to_ptr, 4
    SHE NO SECURE BOOT, 13
                                              Shared Buffer, 12
    SHE RNG SEED, 13
                                              SHE BUSY
    SHE_SEQUENCE_ERROR, 13
                                                  Error codes, 13
    SHE_UNKNOWN_WARNING, 13
                                              she_err_t
Key store, 7
                                                  Error codes, 13
    KEY STORE OPEN FLAGS CREATE, 8
                                              SHE_FATAL_FAILURE
    KEY STORE OPEN FLAGS DEFAULT, 7
                                                  Error codes, 13
                                              SHE GENERAL ERROR
    KEY STORE OPEN FLAGS SET MAC LEN, 8
    KEY STORE OPEN FLAGS SHE, 8
                                                  Error codes, 13
    KEY STORE OPEN FLAGS STRICT OPERATIONSHE_HANDLE_NONE
                                                  Session, 3
                                              she hdl s, 3
    MIN MAC LEN NOT SET, 7
    MIN MAC LEN SET, 7
                                              she hdl t
    she open key store, 8
                                                  Session, 4
                                              SHE_KEY_EMPTY
    SHE_STORAGE_CREATE_FAIL, 8
                                                  Error codes, 13
    SHE_STORAGE_CREATE_SUCCESS, 8
    SHE STORAGE CREATE UNAUTHORIZED, 8
                                              SHE_KEY_INVALID
    SHE STORAGE CREATE WARNING, 8
                                                  Error codes, 13
    SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAULSHE_KEY_NOT_AVAILABLE
                                                  Error codes, 13
                                              SHE_KEY_UPDATE_ERROR
    SHE STORAGE NUMBER UPDATES DEFAULT,
                                                  Error codes, 13
                                              SHE_KEY_WRITE_PROTECTED
KEY_STORE_OPEN_FLAGS_CREATE
                                                  Error codes, 13
    Key store, 8
                                              SHE_MAX_SESSIONS
KEY_STORE_OPEN_FLAGS_DEFAULT
                                                  Session, 3
    Key store, 7
                                              SHE_MEMORY_FAILURE
KEY_STORE_OPEN_FLAGS_SET_MAC_LEN
                                                  Error codes, 13
    Key store, 8
                                              SHE NO DEBUGGING
KEY_STORE_OPEN_FLAGS_SHE
                                                  Error codes, 13
    Key store, 8
                                              SHE NO ERROR
KEY STORE OPEN FLAGS STRICT OPERATION
                                                  Error codes, 13
    Key store, 8
                                              SHE NO SECURE BOOT
MIN MAC LEN NOT SET
                                                  Error codes, 13
    Key store, 7
                                              she_open_key_store
MIN_MAC_LEN_SET
                                                  Key store, 8
```

16 INDEX

```
SHE_OPEN_SESSION_EXCLUSIVE_MASK
    Session, 3
SHE_OPEN_SESSION_FIPS_MODE_MASK
    Session, 3
SHE_OPEN_SESSION_LOW_LATENCY_MASK
    Session, 4
SHE_OPEN_SESSION_NO_KEY_STORE_MASK
    Session, 4
SHE OPEN SESSION PRIORITY HIGH
    Session, 3
SHE_OPEN_SESSION_PRIORITY_LOW
    Session, 3
she_open_utils
    Utils, 10
SHE_RNG_SEED
    Error codes, 13
SHE SEQUENCE ERROR
    Error codes, 13
she_session_hdl_to_ptr
    Session, 4
SHE_STORAGE_CREATE_FAIL
    Key store, 8
SHE_STORAGE_CREATE_SUCCESS
    Key store, 8
SHE_STORAGE_CREATE_UNAUTHORIZED
    Key store, 8
SHE_STORAGE_CREATE_WARNING
    Key store, 8
SHE_STORAGE_MIN_MAC_BIT_LENGTH_DEFAULT
    Key store, 8
SHE_STORAGE_NUMBER_UPDATES_DEFAULT
    Key store, 8
SHE_UNKNOWN_WARNING
    Error codes, 13
Utils, 10
   she_open_utils, 10
```